I claim:

1. A method of operating an access system including a network access server to provide access between a user and a service network, the method comprising the steps of:

providing an authentication server;

generating a challenge using a random sequence without communicating with the network access server;

generating a response to the challenge;

sending the response to the network access server using an authentication protocol;

forwarding the response to the authentication server;

receiving and processing the response indicating whether the user is allowed access to the service network by decrypting the response using a user encrypted private key;

providing access to the service network to the user in response to the authorization generated by the authentication server.

2. The method of Claim 1, wherein the challenge is generated based on time.

3. The method of Claim 1, wherein the challenge is generated based on a non-repeating number sequence.

4. The method of Claim 1, wherein the authentication protocol is an indirect authentication protocol.

5. The method of Claim 1 wherein the authentication protocol is RADIUS.

6. The method of Claim 1 wherein the authentication protocol is TACAS.

7. The method of Claim 1 wherein the authentication protocol is TACAS+.

8. The method of Claim 1 wherein the authentication protocol is XTACAS.

9. The method of Claim 1, wherein the response is generated using public-key cryptographic algorithm and encrypting the challenge with the user's private key.

10. The method of Claim 1, wherein the response is generated using symmetric key cryptographic algorithm and encrypting the challenge with a shared secret.

11. The method of Claim 9, wherein the user's private key is stored in a smart card device.

12. A method of operating an access system including a network access server with an established authentication protocol to provide access between a user and a service network, the method comprising the steps of:

providing an authentication server;

providing a challenge generator;

generating a challenge through a communication channel outside the authentication protocol using a random number sequence using encryption by a user public key;

generating a response to the challenge by decrypting the random number using a user private key;

sending the generated response to the network access server through the authentication protocol and to the challenge generator;

forwarding the response to the authentication server;

receiving and processing the response indicating whether the user is allowed access to the service network by decrypting the response using the user encrypted public key;

providing access to the service network to the user in response to the authorization generated by the authentication server.

13. The method of Claim 12, wherein the authentication protocol is an indirect authentication protocol.

14. The method of Claim 12, wherein the authentication protocol is RADIUS.

15. The method of Claim 12, wherein the authentication protocol is TACAS.

16. The method of Claim 12, wherein the authentication protocol is TACAS+.

17. The method of Claim 12, wherein the authentication protocol is XTACAS.

18. The method of Claim 12, wherein the challenge generator is configured to generate and transmit a challenge query.

19. A software product for providing access between a user and a service network access equipped with a network access server, the software product comprising:

authentication software operational when executed by a processor to direct the processor to generate a challenge without communicating with the network server, encrypt the challenge, receive the user response to the challenge, process the user response to determine if the user is allowed access to the service network based on decrypting the user response and matching the user response with the encrypted challenge, and provide access to the service network to the user in response to the authorization response that allows the user to use the service network; and

a software storage medium operational to store the authentication software.

20. The software product of Claim 19, wherein the user response includes a random number decrypted using a user private key.

21. The software product of Claim 20, wherein the user response includes a non-repeating number sequence decrypted using a user encrypted private key.